

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. – 7. (canceled)

8. (currently amended) A method for providing certificate updates, the method comprises the steps of:

a) generating, by an end user, certificate update subscription information that includes at least identity of ~~a plurality of~~ at least one subscriber subjects subject that the end user is interested in and their associated public ~~[[keys]]~~ key, and receiving the certificate update subscription information from the user, wherein the certificate update subscription information includes at least one current ~~certificates~~ certificate for those subscriber subjects that the end user has a desire to communicate with, at least one of: identity of at least one of subscriber subject, a public key certificate of the at least one subscriber subject, an attribute certificate of the subscriber subject, identity of a certification authority and a cross-certificate;

b) monitoring certificate of the at least one subscriber subject; and

c) when a change occurs to the certificate, providing an indication of the change to the user~~[[,]]~~.

~~the method further comprising receiving an indication of a user replica of the certificate from the user, when the use is on-line;~~

~~determining whether the user replica of the certificate is consistent with server replica of the certificate; and~~

~~when the user replica of the certificate is inconsistent with the server replica of the certificate, providing an indication of the server replica of the certificate to the user.~~

9. (canceled)

10. (canceled)

11. (original) The method of claim 8 further comprises, within step (c), providing the indication as at least one of: an encoded message identifying the change to the public key certificate of the at least one subscriber subject.

12. (original) The method of claim 8 further comprises, within step (b), monitoring the public key certificate by pulling the public key certificate of the at least one subscriber subject from a certification authority.

13. (original) The method of claim 8 further comprises receiving information to change the public key certificate of the at least one subscriber subject.

14. (original) The method of claim 8 further comprises, within step (a) receiving from an end-user or system administrator the public key certificate update subscription information.

15. (previously presented) A method for obtaining public key certificate updates, the method comprises the steps of:

a) generating by a user, certificate update subscription information that includes at least identity of at least one subscriber subject that the end user is interested in and their associated public keys, and providing by the user, the public key certificate update subscription information to a server, wherein the public key certificate update subscription information identifies at least one subscriber subject that the end user is interested in and their associated public keys;

b) monitoring, by the server, public key certificate of the at least one subscriber subject;

c) when a change occurs to the public key certificate, providing, by the server, an indication of the change to the user;

d) while on-line, receiving, by the user, the indication of the change; and

e) determining, by the user, newly updated public key certificate based on the indication of the change.

16. – 23. (canceled)

24. (currently amended) A server of secure communication system, wherein the server comprises:

processing unit;

memory operably coupled to the processing unit, wherein the memory stores programming instructions that, when read by the processing unit, causes the processing unit to (a) generate by a user certificate update subscription information that includes at least identity of at least one subscriber subject that the end user is interested in and their associated public keys, and receive the certificate update subscription information from the user, wherein the certificate

update subscription information for those subscriber subjects that the end-user has a desire to communicate with includes at least one of: identity of at least one of subscriber subject, a public key certificate of the at least one subscriber subject, an attribute certificate of the subscriber subject, identity of a certification authority and a cross-certificate; (b) monitor certificate of the at least one subscriber subject and the certification authority; (c) provide an indication of a change to the user when the change occurs to the certificate. [[; and]]

~~(i) receive an indication of a user replica of the certificate from the user, when the user is on-line; (ii) determine whether the user replica of the certificate is consistent with server replica of the certificate; and (iii) provide an indication of the server replica of the certificate to the use when the user replica of the certificate is inconsistent with the server replica of the certificate.~~

25. (canceled)

26. (canceled)

27. (original) The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to provide the indication as at least one of: an encoded message identifying the change to the public key certificate of the at least one subscriber subject.

28. (original) The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to monitor the public key certificate by pulling the public key certificate of the at least one subscriber subject from a certification authority.

29. (original) The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to receive information to change the public key certificate of the at least one subscriber subject.

30. (original) The server of claim 24 further comprises, within the memory, programming instructions that, when read by the processing unit, causes the processing unit to receive from an end-user or system administrator the public key certificate update subscription information.